A Case for Comprehensive DNSSEC Monitoring and Analysis Tools

Casey Deccio
Sandia National Laboratories

SATIN 2011
National Physical Laboratory, Teddington, UK
Apr 4, 2011

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy’s National Nuclear Security Administration under contract DE-AC04-94AL85000.
DNS objectives and challenges

- **Availability**
  - Responsiveness of authoritative servers upon which name resolution is dependent

- **Consistency**
  - Consistent responses across authoritative servers

- **Integrity**
  - Correctness of data returned by resolvers
DNSSEC implications

● **Availability**
  ● Responsiveness of authoritative servers upon which name resolution is dependent

● **Consistency**
  ● Consistent responses across authoritative servers

● **Integrity**
  ● Correctness of data returned by resolvers

Brings challenges to **availability** and **consistency**

Explicitly addresses **integrity**
Objectives

• **Identify** DNSSEC operational pitfalls
• **Analyze** results of DNSSEC deployment survey to determine problem pervasiveness
• **Propose** solutions for improving DNSSEC availability and consistency
Outline

- DNSSEC workings
- DNSSEC challenges
- DNSSEC survey and results
- Solutions
DNS Security Extensions (DNSSEC)

- RRsets signed with zone’s private key(s)
- Signatures covering RRsets returned by server as RRSIGs
- Public keys published in zone data as DNSKEYs
- Resolver validates response
  - If authentic: Authenticated data (AD) bit is set
  - If bogus: SERVFAIL message is returned

Diagram:
- Query: www.bar.com/A ?
  - Answer: 192.0.2.16
- Query: bar.com/DNSKEY ?
  - Answer: DNSKEY...
  - Answer: RRSIG
- Query: www.bar.com/A ?
  - Answer: 192.0.2.16
  - AD

stub resolver recursive/validating resolver authoritative server
Scalable authentication via a chain of trust

- DNSKEY must be authenticated
- Resolver must have some notion of trust
- Trust extends through ancestry to a trust anchor at resolver
- DS resource record – provides digest of DNSKEY in child zone
Backwards compatibility…
kind of

- If no secure link exists between parent and child, referring (parent) server must prove non-existence of DS RR
- NSEC/NSEC3 resource records provide authenticated denial of existence
- Child zones of insecure delegations may be unsigned or signed ("islands of security")
DNSKEY roles

- **Secure entry point (SEP)**
  - Provides trusted entry into zone (via DS or trust anchor)

- **Two-key setup:**
  - **Key-signing key (KSK)**
    - Signs only DNSKEY RRset
    - Authenticates other DNSKEYs
    - Typically functions as SEP
  - **Zone-signing key (ZSK)**
    - Signs (only) zone data
DNSSEC validation status

- **Secure** – unbroken chain from anchor to RRset

(Image from http://dnsviz.net/)
DNSSEC validation status

- **Insecure** – chain that securely terminates (i.e., insecure delegation)

(Image from http://dnsviz.net/)
DNSSEC validation status

- **Bogus** – broken chain

(Image from http://dnsviz.net/)
Outline

- DNSSEC workings
- DNSSEC challenges
- DNSSEC survey and results
- Solutions
DNSSEC challenges – maintenance

● More maintenance required than for unsigned zones
  ● RRSIG refreshing
  ● DNSKEY rollovers
    ● ZSK rollovers – non-SEP, self-contained
    ● KSK rollovers – SEP requires interaction with parent or trust anchor
  ● Algorithm changes
DNSSEC challenges – product support

- DNSSEC implementations are “new”
- There are varying levels of DNSSEC support on authoritative servers
  - Support for DNSSEC RR types
    - Accept DNSSEC RR types (DNSKEY, NSEC, etc.)
  - DNSSEC protocol support
    - Return RRSIGs, NSEC, DS, appropriately
  - NSEC3 support
    - Return NSEC3s appropriately
DNSSEC challenges – dependencies

- Dependence on other zones and servers increased for authentication
  - Proper DNSSEC support by authoritative servers
  - Ancestor zones
  - Targets of aliases

Query: www.bar.com/A ?
Answer: 192.0.2.16
Data tampering or misconfiguration?

Query: www.bar.com/A?

SERVFAIL

stub resolver  recursive/validating resolver  authoritative servers
Inconsistent responses

- Inconsistent responses due to stale zone data or insufficient DNSSEC support
- **Possible** failure vs. **certain** failure
- “Smart” resolver implementations exist, but cannot be depended upon
  - Load balancing
  - Failover

![Diagram](Image)
Outline

- DNSSEC workings
- DNSSEC challenges
- DNSSEC survey and results
- Solutions
DNSSEC deployment survey

- Polled ~2,200 production signed zones over a five month time frame (June – Nov 2010)
- Validation of SOA RR analyzed every four hours, anchored at ISC DLV or root zone (after July 2010)
- Identified misconfigurations observed in two or more consecutive polls (4+ hours)
Survey breakdown by TLD

Zones
Zones with misconfigurations

gov  cz  org  br  se  arpa  com  net  dk  edu  de  be  uk  eu  other
Misconfigurations by type

- RRSIG - invalid dates
- Missing RRSIG
- RRSIG - bogus sig
- Missing DNSKEY
- DS mismatch

- Certain failure
- Possible failure
Event duration

- RRSIG - invalid dates
- Missing RRSIG
- RRSIG - bogus sig
- Missing DNSKEY
- DS mismatch
Event repetition

![Graph showing event repetition]

- RRSIG - invalid dates
- Missing RRSIG
- RRSIG - bogus sig
- Missing DNSKEY
- DS mismatch
Outline

- DNSSEC workings
- DNSSEC challenges
- DNSSEC survey and results
- Solutions
Desired properties of analysis tools

- Multi-dimensional
  - Hierarchical – along chain of trust
  - Lateral – across authoritative servers
  - Diverse – across anycast instances

- Dependency-aware
  - CNAME, MX, NS target dependencies

- Aggregation capable
  - Highlight anomalies

- Targeted
  - Cache analysis
  - Source consciousness
Monitoring

- **Active monitoring**
  - Periodic, based on:
    - Usage
    - Level in hierarchy (e.g., TLD)
    - TTL, RRSIG expiration
    - Past experience
  - On-demand
- **Passive monitoring**
  - Validation failures
- **Alerts**
  - Subscription based
  - Targeted
Interactive maintenance

- Maintenance tools should be aware of status servers
  - RRSIG status after refresh
  - DNSKEY status after rollovers
  - DNSSEC support
Expired RRSIG
Expired RRSIG

DS referring to “published only” DNSKEY
Missing DNSKEYs from some servers

Missing RRSIGs from some servers

nasa.gov
(2011-02-23 16:55:30 UTC)
Two versions of same key- one valid, one invalid
RRSIG covering NSEC RR returned by fraction of servers was invalid
Some servers not returning NSEC(3) RRs
No servers returning NSEC RRs
Summary

- DNSSEC introduces challenges to availability and consistency
- Monitoring and analysis will help administrators learn, troubleshoot, and be alerted of issues in DNSSEC deployments
Acknowledgements

- Jeff Sedayao, Krishna Kant at Intel Corporation
- Prasant Mohapatra at UC Davis
Questions?

- ctdecci@sandia.gov